# 端末間の近距離通信を使ったFederated Learningによる観光オブジェクト認識モデルの参加型学習法とその評価

冨田 周作[1,2]　中村 優吾[3]　諏訪 博彦[1,2]　安本 慶一[1,2]

**概要**：観光地の多様なコンテキストの認識には，観光客が持つ写真等のデータを使って学習した認識モデルが必要となるが，そのためには個人データに含まれるプライバシに配慮する必要がある．この問題は，Federated Learning で解決できる可能性がある．しかし，Federated Learning は，十分な計算能力を備えた集約サーバの設置が前提であり，モデル構築のために，観光客端末と集約サーバ間の通信および端末上のモデル更新が高頻度に行われると，端末での通信コスト（電力・通信費等）が大きくなり観光客の不満が生じてしまう．本研究では，観光客端末間での近距離直接通信を活用した Federated Learning に基づくモデル構築の手法を提案する．提案手法では，すれ違った他の観光客が持つモデルの重みパラメタを受信し自分のモデルに統合する．提案手法では, 端末同士がすれ違った際に，性能向上に有効かどうかを，モデルの学習度合いを表す少ない情報の交換を行うことで事前判定し，有効と判断された場合にのみ，モデルパラメタの受信・統合を実行することで，限られた通信回数および少ない消費電力で自身のモデル性能を効率的に向上させる．実在する観光地を想定し，そこでの実際のモバイルユーザのトレースデータを使ったシミュレーション実験を行い，10 オブジェクトを識別する CNN モデル（初期精度は 12.22%）の識別精度向上度合いを，モデル統合回数を 40 回に制限した上で評価した．結果，すれ違った相手とある確率でモデル交換するゴシッププロトコルに基づいた手法では 1%程度（平均精度 12.45%）の精度向上に留まったのに対し，事前判定で統合の有無を決定する提案手法は，平均精度を 172%（平均精度 33.24%）と大きく向上可能なことが分かった．

## 1. はじめに

近年，観光サービスにおける AI の活用が促進されている [1]．例として，ユーザが SNS に投稿した情報や行動履歴から観光スポットの推薦や観光情報を提供するスマートフォンアプリ「Deaps」[2] がある．また，欧州で提唱されたスマートツーリズムは，高度な ICT を活用したサービスを統合することで，新たな観光体験を創出することが目指されている [3]．国土交通省観光庁による令和３年版観光白書[*1]では，観光のトレンドの変化についての調査結果を報告しており，近年，滞在型観光，分散型旅行，近場での旅行，オンラインツアーといった新たな多様な旅行スタイルが人気になっていることが報告されている．このように，観光客や観光スタイルの多様化に対応するために，観光 AI の開発・活用が今後加速していくと予想される．観光 AI の主要な機能として，観光地のコンテキスト（混雑度やイベントの有無，天気，景観など）をリアルタイムに認識することが挙げられる．観光地のコンテキスト認識には，物体認識モデルを使用し，映像や写真から認識した物体群から，総合的にコンテキストを推定する方法が有望である．観光地は固有の観光オブジェクト (鹿などの野生動物，寺社仏閣といった建造物，桜や紅葉と言った景観，その他文化遺産等) を含む．そのため，それら多種多様な物体の認識モデルの構築には多様で膨大なデータを使った学習が必須である．そのデータの収集には，大企業等が保有するビッグデータや個人のスマートフォンに保存されている写真・映像等の活用が望ましい．しかし，プライバシ等の問題でこれらのデータを使ったモデルの学習は難しいのが現状である．

Google が提案した Federated Learning citeMcMahan は，上記の問題を解決できる可能性がある点で近年大きな注目を集めている．Federated Learning は，各端末が所持しているデータをその端末上で学習し，モデルのみを集約サーバに集約・統合することで間接的に全端末のデータを学習する．モデルの重みパラメタや勾配のみが外部（サーバ）に送信され，学習データは送信されないため，プライバシ情

[1] 奈良先端科学技術大学院大学，Nara Institute of Science and Technology
[2] 理化学研究所 革新知能統合研究センター (AIP), RIKEN, Center for Advanced Intelligence Project (AIP)
[3] 九州大学，Kyushu University
[*1] https://www.mlit.go.jp/kankocho/news02$_0$00447.*html*

報が漏洩しにくいという特徴を持つ．Federated Learningを観光オブジェクト認識モデルの構築に適用する場合，観光客の写真が学習対象となる．Federated Learningに参加する観光客が多い程，多様な観光オブジェクトに認識するモデルが構築される．しかし，集約サーバの維持運用コストに加え，観光客端末のサーバとの高頻度で大容量の広域無線通信が必要となり，通信コスト（通信費，消費電力等）が増加する．上記を踏まえ，Federated Learningに基づいて観光オブジェクト認識モデルを構築するにあたり，（課題1）コストが高い広域無線通信および集約サーバを使用しないこと，（課題2）限られたモデル更新回数（限られた通信コスト）で統合後モデルの精度が最大化されるようモデル統合相手を選ぶこと，の2つの課題を設定する．

本研究では，上記課題1，2を解決する手法を提案する．課題1に対しては，観光客端末間の近距離直接通信（WiFi DirectやBLEなど）によりモデルパラメタを送受信し統合する．課題2に対しては，モデルパラメタの通信前に少ない情報の交換により更新後のモデルの精度を予測し，精度向上の可能性が高い相手とパラメタの送受信を行う．

課題1に対して，著者らは，本研究の先行研究として，端末間の直接通信を前提としたモデル更新手法 [4] を提案している．モデルの重みパラメタを平均化するFedAvg [5] を基とした幾つかのモデル統合法を提案し，様々な学習度合いのモデルの組合せに対し，単純平均で統合する場合に精度が向上する組合せが最多になること，統合前の2モデルの精度から統合後モデルの精度が予測可能であることを示した．

課題2の解決は本稿の主題であり，課題1に対する先行研究の結果を活用して解決する．具体的には，先行研究 [4] の内容に基づいて，観光客の移動を考慮したモデル更新アルゴリズムを提案する．提案アルゴリズムでは，観光客がすれ違う際に互いのモデルの認識精度の情報のみを交換し，その情報から統合後の精度を予測する．そして，統合後の精度が，設定した閾値より高い場合，モデルの重みパラメタを受け取り単純平均で統合する．これにより，精度向上に有用なモデルのみを統合することができ，各端末の総合的な消費電力を抑制する．

提案アルゴリズムの評価のため，実在する観光地における実際のモバイルユーザのトレースデータを使ったシミュレーションを実施した．シミュレーションでは，各ユーザに精度が異なる初期モデル（10オブジェクトを認識するCNNモデル）を割り当て，すれ違いが発生したユーザ間でモデル更新を試みる．モデル統合回数を40回に制限し，ゴシッププロトコルに基づいた手法（出会った相手とある確率でモデル交換する）と本提案アルゴリズムを適用したシミュレーションをそれぞれ実施し比較した．結果，初期モデルの平均精度12.22%に対し，ゴシップ手法では全体の平均精度が12.45%（1%の向上）でほぼ変化しなかったのに対し，提案アルゴリズムでは33.24%（172%の向上）となり，提案手法の有効性が示された．

本稿の構成は以下の通りである．2章では，本研究に関連する既存研究について概説する．3章では，本研究の想定環境およびシナリオを説明し，問題設定を行う.4章で提案手法を述べ，5章ではシミュレーション実験と評価，6章でその考察を述べる．7章で，本稿のまとめを述べる．

## 2. 関連研究

本章では，端末間の通信を活用したFederated Learningによるモデル構築手法の既存研究について述べる．

### 2.1 近隣端末間のFederated Learning

Lee [6] らはモバイル端末間の通信のみでFederated Learningを実施する手法を提案している．Leeらの提案したOpportunistic Federated Learning [6] では，モバイル端末が移動中に他端末と出会った際，モデルを相手端末に送信しその内部データを学習させる．相手データ学習後にその勾配を返し，相互の学習で得られた勾配の平均でモデルを更新する．この処理が同端末間で複数回実行され，相手データが学習される．また，自身のモデルに適した相手を選択するために自身の認識対象のラベルと相手の所持データのラベルが類似した相手に対し学習処理が行われる．この手法に対し，本研究では，同端末間での通信コストを抑制するために勾配ではなくモデルの重みパラメタを使用する．また，相手の選択方法として，所持データのラベルではなく相手のモデル性能に基づいて端末を選択する．

Leeらの実験では，画像分類タスクにおいて認識対象のラベルが異なるモデルを多数使用し，モバイル端末の移動データを生成して任意のモデルを訓練する実験が行われた．端末間の近距離通信に基づくため，広域無線通信による電力消費が抑制される．しかし，入力データに対する勾配を平均するFedSGD [5] を更新手法として採用している．そのため，相互の所持データに対する勾配が更新に必要となり，データ数が多い程勾配の通信回数が増加する．また，十分な更新には多端末との通信が必要となり，近距離通信における電力消費も多くなる．そのため，Federated Learningで必要となる通信量を削減する研究 [7] が行われている．本研究では，通信コスト抑制とモデル精度の向上を両立する手法を検討しており，通信コストを考慮する点でLeeらの手法と異なる．

### 2.2 サーバを部分的に用いるFederated Learning

Chen [8] らは，本来のFederated Learning [9] において必須となる集約サーバへの依存度を低下させる手法を提案している．この手法では，集約サーバへのアクセスが困難な端末も訓練への参加が可能になるように，互いに近距離に位置するエッジ端末間のローカルネットワークでモデル

を集約している．各端末にも集約サーバと類似した処理を実行させることで，集約サーバが全てのエッジ端末を網羅できない状態でも全体の端末のモデルの訓練を可能としている．しかし，この手法は近隣の全エッジ端末と通信するため，端末数の規模に応じて通信回数が増加する．そのため，モデル集約の際の電力消費等のコストが増大する．

### 2.3 ブロックチェーンを用いた Federated Learning

Kim [10] らは，ブロックチェーンによる Federated Learning（BlockFL）を提案している．BlockFL では，集約サーバ内でのグローバルモデル構築が必要ない．集約サーバをブロックチェーンで代用し，各端末のモデル更新情報を記録したブロックを生成する．そのブロックの情報から各端末内で共通のグローバルモデルを構築し，再度ローカルで学習を繰り返す．これにより，各ローカル端末がグローバルモデルを持つため，集約サーバの必要性が無くなる．しかし，グローバルモデル構築には，全端末のモデル更新後のパラメタの差分が必要であり多数端末が参加する場合，グローバルモデル構築のためのパラメタの差分が揃うまで時間がかかる．そのため，全体の処理時間が長くなる．

### 2.4 既存手法に対する本研究の位置づけ

基本的に Federated Learning はモデルを集約するサーバが必要となるが，これらの関連研究のように集約サーバへの依存性を低減または皆無にする手法も複数提案されている．しかし，端末間のネットワークの固定が必要な手法や，間接的に集約サーバが必要となる手法，訓練全体で多くの端末との複数回の近距離通信が必要な手法等，通信環境が比較的安定する中での手法が多く，通信環境が全体的に不安定な環境での適用は困難である．本研究で提案する手法では，端末間の直接通信により通信環境に依存しない Federated Learning を実施し，また，モデル統合回数を制限し，その制限のもとでモデルの精度の最大化を目的としている点で，既存研究と異なる．

## 3. 問題設定，課題とアプローチ

本章では，想定環境と問題設定，ユースケースシナリオについて述べる．

### 3.1 想定環境と問題定義

本研究では，Federated Learning に基づいて観光オブジェクト認識モデルをユーザ参加型で構築するための手法の実現を目指している．**表 1** に想定環境で登場する要素およびその内容を示す．

想定環境とする観光エリアの集合を $A$ とする．それぞれの観光エリア $a \in A$ には認識したい観光オブジェクトの集合 $O_a$ が存在している．$O_a$ はオブジェクト（動物，群衆，屋台など）や固定されたオブジェクト（建物，鳥居，樹木など）が該当する．$A$ の観光エリア間及び内部には，複数の観光客が滞在及び移動をしており，各観光客はスマートフォン等のモバイル端末を所持する．これらの集合を $C_{mobile}$ とする．各観光客はモバイル端末を 1 台のみ持つと想定する．また，観光エリアにはサイネージ等の固定端末も配置されており，その集合を $C_{stationary}$ とする．想定環境 $A$ 内に存在する端末の集合 $C$ を式 (1) で表記する．

表 1: 想定環境に登場する記号一覧

| 要素 | 定義 |
|---|---|
| $A$ | 観光エリアの集合 |
| $A_c$ | 認識能力を強化したいエリア |
| $O_a$ | $a \in A$ 内の認識オブジェクトの集合 |
| $O_c$ | 認識強化オブジェクトの集合 |
| $C_{stationary}$ | 固定端末の集合 |
| $C_{mobile}$ | 移動端末の集合 |
| $C$ | 全端末の集合 |
| $R$ | 端末が通信可能な範囲 |
| $D_c$ | 端末 c が持つデータの集合 |
| $D$ | 全データ |
| $M_c$ | 端末 $c$ が持つモデル |
| $W_c$ | モデル $M_c$ の重みパラメタ |
| $T$ | 想定環境内の時間 $t$ の集合 |
| $pos(c,t)$ | 端末 $c$ の時刻 $t$ の位置 |
| $cn(c,c',t)$ | 時刻 $t$ での端末 $c$，$c'$ のコンタクト |
| $CN$ | 全端末のコンタクト |

$$C = C_{stationary} \cup C_{mobile} \tag{1}$$

想定環境におけるタイムスロット (時刻) の集合を $T$ とすると，端末 $c \in C_{mobile}$ は，$t \in T$ 毎に位置が変わる．$c$ の $t$ での位置を $pos(c,t)$ と表記する．$t$ における $c, c'$ が互いに通信可能な範囲 $R$ にいる場合，それらが互いにコンタクトしているとみなし，そのコンタクトを $cn(c,c',t)$ とする．全コンタクトの集合 $CN$ を式 (2) で表す．

$$CN = \bigcup_{c,c' \in C, t \in T} cn(c,c',t) \tag{2}$$

各モバイル端末 $c \in C_{mobile}$ は学習データを所持しているが，固定端末 $c \in C_{stationary}$ は所持しない．各端末 $c \in C$ の所持データを $D_c$ と表記すると，$c \in C_{mobile}$ では $D_c \neq \emptyset$，$c \in C_{stationary}$ では $D_c = \emptyset$ となる．想定環境内の全データを $D$ として式 (3) で定義する．

$$D = \bigcup_{c \in C_{mobile}} D_c \tag{3}$$

固定端末 $C_{stationary}$ を除く各端末 $c \in C$ は自身のデータ $D_c$ で学習した観光オブジェクト認識モデル $M_c$ を所持しており，$M_c$ の重みパラメタ $W_c$ を他の観光客の重みパラメタ $W_{c'}$ と統合する．各端末 $c$ が持つモデル $M_c$ には認

識したい観光エリア $A_c \subseteq A$ が設定されおり，その観光オブジェクトの集合 $O_c$ を式 (4) として定義する．

$$O_c = \bigcup_{a \in A_c} O_a \tag{4}$$

観光客のコンタクトに関して，時刻 $t$ で 1 対 1 の観光客のコンタクトが発生した場合，両者の端末間で重みパラメタの通信が可能とする．任意の端末が複数の端末と通信が可能な状況にある場合においては，その中の 1 つと通信する．これを二値変数 $x_{cn(c,c',t)}$ を用いて式 (5) として定義する．式 (5) では，$x_{cn(c,c',t)}$ は端末間の通信の有無を表す変数であり，端末 $c$ と他端末 $c'$ との間で通信する場合は $x_{cn(c,c',t)} = 1$，通信しない場合は $x_{cn(c,c',t)} = 0$ となる．

$$\sum_{cn(c,c',t) \in CN, c \neq c'} x_{cn(c,c',t)} \leq 1, \forall c \in C, \forall t \in T \tag{5}$$

本研究では消費電力抑制も考慮するため，各端末の重みパラメタの通信可能な回数を $L$ と表記する．この制約を式 (6) として表現する．

$$\forall c \in C, \sum_{cn(c,c',t) \in T} x_{cn(c,c',t)} \leq L \tag{6}$$

本研究では，各端末の通信回数の最小化とモデルの改善度合いの最大化のために精度向上に効果的なコンタクトの選択が必要となる．$M_c$ に $M_{c'}$ のパラメタを統合することによるモデル精度の改善度合いを $Improve(M_c, M_{c'})$ として，本問題の目的関数を式 (7) に表す．

$$\begin{aligned} Maximize \sum_{c \in C} \sum_{c' \in C\{c\}} \sum_{t \in T} \sum_{cn(c,c',t) \in CN} \\ x_{cn(c,c',t)} \cdot Improve(M_c, M_{c'}) \\ subject\ to\ (5), (6) \end{aligned} \tag{7}$$

### 3.2 想定シナリオ

上記の想定環境に基づく想定シナリオ [11] について述べる．想定シナリオでは奈良県内の観光エリア (奈良公園, 東大寺，春日大社) が対象としている．各観光エリアには各エリアを特徴付ける観光オブジェクトが存在している．これらの集合を以下の $O_{奈良公園}$,$O_{東大寺}$,$O_{春日大社}$ とする．

$O_{奈良公園}$ = { 牡鹿, 牝鹿, 小鹿, 鹿煎餅の売店,...}
$O_{東大寺}$ = { 仏像, 池, 鯉, 桜, 牡鹿, 牝鹿...}
$O_{春日大社}$ = { 藤, 鳥居, 池, 鯉, 社,...}

また，観光エリア内では観光客が所持するモバイル端末 $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9$ が移動および滞在し，互いの観光オブジェクト認識モデルの重みパラメタを通信する．モデルのパラメータは少なくとも数 MB のサイズとなるため，ユーザ同士がすれ違う短時間で通信を完了するために WiFi-Direct を使用する．

各モバイル端末のユーザは，観光前に自宅等の通信状態が安定する場所で，限定数の観光オブジェクトのデータについて訓練済みのベースモデルをダウンロードしている．各ユーザはこのベースモデルに自身でアノテーションしたデータを訓練させてから観光を始める．観光中にもデータ増加が予想されるため，観光後はその追加データの訓練を自宅や充電スポット等の電力確保が可能な場所で行う．観光前に自身の所持データがないのユーザについてはベースモデルのダウンロード後に観光を開始する．各観光エリアの敷地内にはサイネージが 1 台設置されており，$c_{奈良公園}$,$c_{東大寺}$,$c_{春日大社}$ がある．これらは学習データは持たないが，観光エリア内の一部のオブジェクトに対して認識可能なモデルを持つとする．

**図 1** に前述の端末群によるシナリオを示す．想定シナリオでは端末 $c_1$ の観光客が近鉄奈良駅から奈良公園，東大寺，春日大社の順に観光し，その途中で他の観光客とコンタクトする．これらのコンタクトを活用し他のモデルにアクセスしながら $c_1$ の観光オブジェクトモデルを更新する．また，$c_1$ の他のモバイル端末やサイネージにおいても同様に，コンタクトが生じた場合に相手のモデルにアクセスし更新を行う．想定シナリオでは，それぞれの端末が他の端末とのコンタクトを活用してモデルを更新を繰り返す．

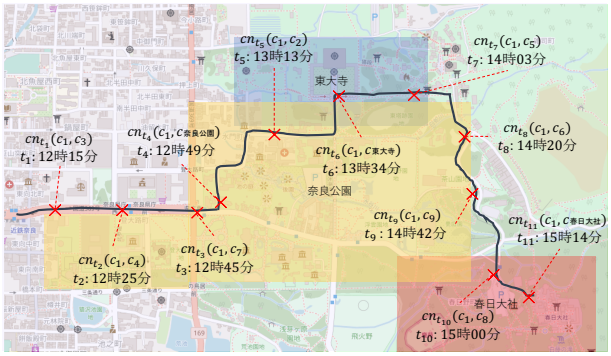



図 1: $c_1$ と各デバイスのコンタクト

### 3.3 課題とアプローチ

#### 3.3.1 本研究の課題

本研究の想定環境・シナリオでの観光オブジェクト認識モデル構築について以下の 2 点の課題が挙げられる．

前述の想定環境に関して，モデル更新に従来の Federated Learning [5][9] を活用する場合，全端末がアクセス可能な集約サーバが必要となる．しかし，観光客の数が膨大になると，集約サーバやそのアクセスに必要なネットワークに負荷が集中する．そのため，従来の集約サーバを活用する手法では，学習可能なモデル数の制限や更新頻度の低下が発生する．これらの制限を抑制するには，**（課題 *1*）集約サーバを経由しない他端末へのアクセスとモデル更新**が必

要となる．

また，本研究では観光オブジェクト認識モデルとして CNN モデルによる画像分類モデルを採用している．CNN モデルは数十 MB 以上のデータである場合が多いためモデル更新で生じる通信の消費電力も大きい．Lee [6] らは，端末間での訓練で直接通信を複数回実行するため通信処理で多くの電力を消費する．観光客は常に端末の充電が可能であるとは限らないため，端末の電力消費抑制が求められる．そこで，**（課題 *2*）モデルの重みパラメタの通信回数を最小限に抑えながら精度を最大にする手法**が必要である．

#### 3.3.2 課題へのアプローチ

**課題** *1* に対して，他の端末のモデルにアクセスする方法として，端末間で直接通信をする方法（WiFi Direct や BLE の使用を想定している）が挙げられる．端末での直接通信を主なアクセス方法とすることでネットワークや集約サーバへの負荷が減り，より多くの観光客がモデルの訓練に参加できると考える．

**課題** *2* に対して，最小の通信で最大の精度を得る方法として，統合後のモデルの精度の予測を挙げる．精度予測により，統合後の精度が向上するモデルが選択できるため，通信対象の選択が可能となる．また，モデル統合においても，精度向上に効果的な統合方法を活用することで，モデルの精度をより少ない通信回数で最大化できると考える．

## 4. 提案手法

本研究の課題となる**課題** *(1)*，*(2)* を解決する手法として，ユーザの端末間での直接的な通信を活用した Federated Learning に基づくモデル構築の手法を提案する．本章では，その提案手法について述べる．

### 4.1 重みパラメタの更新処理

本研究で想定するモデル更新の概略図を**図 2** に示す．本提案手法では他端末とコンタクトしたタイミングで相互の端末間で通信し，モデルの重みパラメタを取得する．パラメタの取得後，自らのパラメタに対して Federated Learning に基づいた方法で統合する．Federated Learning のモデル統合方法には，主に FedSGD [5] と FedAvg [5] が提案されている．FedSGD では，モデルへの入力に対する勾配の平均を計算するため，データ数に応じて集約サーバとの通信回数が増加する．一方で FedAvg は，各端末のデータ学習後の重みパラメタを集約し平均するため，FedSGD と比較して通信回数が少ない．そのため**課題** *1* に関して，本研究では FedAvg に基づく統合方法を採用した．統合方法としては，本研究の先行研究 [4] で最も良い結果が得られた，重みパラメタを単純平均する方法を使用する．図 2 の更新例に示すように，コンタクト相手のモデルの重みパラメタを受信し，自身の分と単純平均で統合した後で，そのパラメタを自身のモデルに適用する．

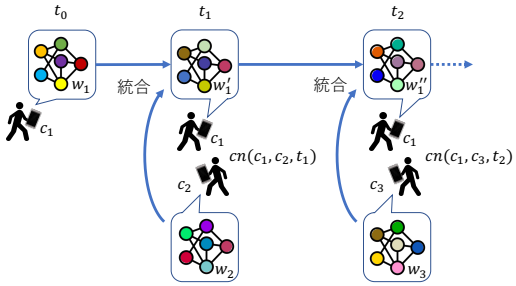



図 2: モデルの重みパラメタ統合の更新例

### 4.2 統合対象の選択方法

本研究の**課題** *2* に関して，統合後の精度予測によって，統合対象を精度向上に有効なモデルに限定し精度の最大化ができると述べた．本節では，精度向上に有効なモデルの選択方法を提案する．統合対象の選択には，オブジェクト認識モデルとは別に，統合後の精度変化 (向上または低下) を予測するモデルを使用する．端末間のコンタクト時に精度変化予測モデルを使用し，精度向上が予測された場合，相手の重みパラメタを統合対象として選択する．精度変化予測モデルにより，精度向上に有効なモデルの選択が可能となる．先行研究 [4] では，自身と相手のモデルの精度から統合後のモデルの精度予測が可能になることが示唆された．そのため，精度変化予測モデルの入力をコンタクトした 2 端末間のオブジェクト認識モデルの精度とする．2 端末間での精度共有にも端末間の直接通信を活用するが，モデルパラメタと比較し非常に小さいデータとなるため，精度共有時に消費する電力は考慮しないものとする．

### 4.3 モデル更新アルゴリズム

上記の手法によるモデル更新アルゴリズムを **Algorithm 1** に示す．Algorithm 1 は，任意の端末 $c$ が別端末 $c'$ とコンタクトした際の $c$ 内の処理を表す．Algorithm1 では，時刻 $t$ における重みパラメタ $W_c^t, W_{c'}^t$ とその精度 $Q_c^t, Q_{c'}^t$ および通信回数上限 $L_c^t$ を使用する．また，1 行目で最初に全端末 $C$ の精度分布を取得[*2]しており，その分布から通信相手に選ぶモデルの精度の閾値 $threshold$ を決定する．2 行目で自身の精度 $Q_c^t$ と通信可能回数 $L_c^t$ から，$c$ が $c'$ の重みパラメタを受信できる回数 $receive$ と，$c'$ からパラメタの要求に対し送信できる回数 $transmit$ を決定する．5 行目において観光客のコンタクト $cn(c, c', t)$ が発生を判定し，6 行目で精度変化予測モデル $accuracyRegressor$ で統合後の精度 $predictAcc$ を予測する．その値が $threshold$ を超えた場合，9 行目で相手 $c'$ から重みパラメタを受信し単純平均で統合・更新し次の 10 行目で $receive$ を 1 つ減らす．超えない場合は $threshold$ を下げる．17 行目で統合後パラメタ $W_c^{t+1}$ のモデルの精度が $threshold$ または統合前の

[*2] 各端末のモデル精度は，モバイルアプリを介してクラウドサーバに定期的にアップロードされると想定している．

**Algorithm 1** モデル更新アルゴリズム

**Require:** $\{W_c^t, W_{c'}^t, Q_c^t, Q_{c'}^t, L_c^t | c, c' \in C, t \in T\}$
**Ensure:** $W_c$ that obtained other $W_{c'}$.
1: $threshold \leftarrow determinThreshold(getAllAccuracy(C))$
2: $receive, transmit \leftarrow limitConfig(Q_c^t, L_c^t)$
3: $continueTour \leftarrow true$
4: **while** $continueTour$ **do**
5:  **if** $cn(c, c', t)$ **then**
6:  $predictedQ \leftarrow Q_c^t + accuracyRegressor(Q_c^t, Q_{c'}^t)$
7:  **if** $predictedQ > threshold$ **then**
8:  **if** $receive > 0$ **then**
9:  $W_c^{t+1} \leftarrow (W_c^t + W_{c'}^t)/2$
10:  $receive \leftarrow receive - 1$
11:  **end if**
12:  **else**
13:  $threshold \leftarrow downThreshold(Q_c^t)$
14:  $continue$
15:  **end if**
16:  $mergedQ \leftarrow evaluate(W_c^{t+1})$
17:  **if** $(mergedQ > threshold) \vee (mergedQ > Q_c^t)$ **then**
18:  $threshold \leftarrow upThreshold(Q_c^t)$
19:  **else**
20:  $threshold \leftarrow downThreshold(Q_c^t)$
21:  **end if**
22:  $Q_c^{t+1} \leftarrow mergedQ$
23:  **end if**
24:  $continueTour \leftarrow decideContinueTour(c)$
25:  **if** $continueTour = false$ **then**
26:  break
27:  **end if**
28:  $L_c^{t+1} \leftarrow receive + transmit$
29:  $receive, transmit \leftarrow limitConfig(Q_c^{t+1}, L_c^{t+1})$
30: **end while**

精度 $Q_c^t$ より高いかを判定し，高い場合は $threshold$ を 18 行目で上げて低い場合は 20 行目で下げる．更新処理後は，28 行目で残りの通信可能回数 $L_c^{t+1}$ を更新し，統合後の精度 $Q_c^{t+1}$ と残りの通信回数 $L_c^{t+1}$ から $receive$ と $transmit$ を 29 行目で再設定する．端末 $c$ の観光客が観光を終えるまでコンタクト時にこれらの処理を繰り返す．

## 5. シミュレーション実験

前章の提案手法に対して，人の移動データに基づくモデル更新シミュレーションを実施した．本章では，シミュレーション内容およびその評価について述べる．

### 5.1 シミュレーション実験の概要と評価方法

前章のモデル更新アルゴリズムによるモデルへの影響の評価のために，前節の人流データと精度変化予測モデルを用いて各ユーザのモデル構築シミュレーションを実施した．本シミュレーションの概略図を**図 3** に示す．図 3 のように，各時刻における全ユーザに対して，コンタクトが生じたユーザ間で Algorithm 1 を適用しモデル更新を実行する．モデルは CNN での画像分類モデルを使用し，シミュレーション内のモデル更新では，相互の重みパラメタを単純平均で統合した．本実験でのモデル更新アルゴリズムでは $threshold$ を全体のモデル精度の中央値に設定し，中央値よりも高い精度のモデルの場合はその精度に設定した．$downThreshold$ 関数に関しては，関数が実行された時点での精度の 0.9 倍，$upThreshold$ 関数については 1.1 倍になるよう $threshold$ を設定している．シミュレーション開始時やモデル更新後の $receive$ と $transmit$ の設定方法としては，$transmit$ がモデルの精度に比例して変化するようにしており，通信可能回数と $transmit$ の差を $recieve$ とした．また，提案手法の他に，モデル通信・更新を実施するコンタクトを 10%の確率でランダムに選択する手法でのシミュレーションも実行し，提案手法と比較した．

表 2: 抽出オブジェクト

| | |
|---|---|
| パターン 1 | イルカ，ライオン，山，ヤシ，橋，紅葉，平野，オレンジ，路面電車，城 |
| パターン 2 | きのこ，高層ビル，ラクダ，ロケット，松，家，蘭，チンパンジー，ランプ |
| パターン 3 | 観賞魚，雲，蜂，アライグマ，ウサギ，狼，恐竜，リス，カップ，バラ |

これら 2 つの手法のシミュレーションを各コンタクトに対して時系列順に実行した．また，モデルは約 58.9MB のデータであり 18 回送信または受信すると約 1GB 通信したことになるため，通信量を送信と受信合わせて 2GB，多くても 2.5GB 以内に収まるように通信回数上限を 40 回にした．提案手法では通信可能回数を 40 回，出会った相手とある確率でモデル交換するゴシッププロトコルに基づいた手法では受信と送信の回数をそれぞれ 20 回とした．シミュレーション後，全モデルの平均精度を求め，その変化を評価した．実験では，本研究で想定する観光写真データの代わりとして，動物や自動車等の 10 種類のオブジェクトで構成される cifar10[*3]を使用した．

### 5.2 人流データ

シミュレーション実験では株式会社 Agoop が提供する「ポイント型流動人口データ」[12] を使用した．2020 年 10 月 31 日から 2020 年 11 月 30 日までの 6 時から 18 時の時間帯での**図 4** のエリアのトレースデータから観光客と思われるユーザを抽出し，1,900 人分のデータを得た．日毎におけるユーザ数が少なく 2 日以上に渡るユーザの追跡ができないので，これら 1 ヶ月分のデータを 1 日のデータとして扱った．また，各ユーザの座標に対しその半径 50m 以内に別ユーザがいた場合コンタクトしたとみなし，時系列に沿ったコンタクトのログデータを作成した．

### 5.3 精度変化予測モデルの構築

先行研究 [4] では，自身と相手のモデル統合後の精度向

[*3] https://www.cs.toronto.edu/ kriz/cifar.html

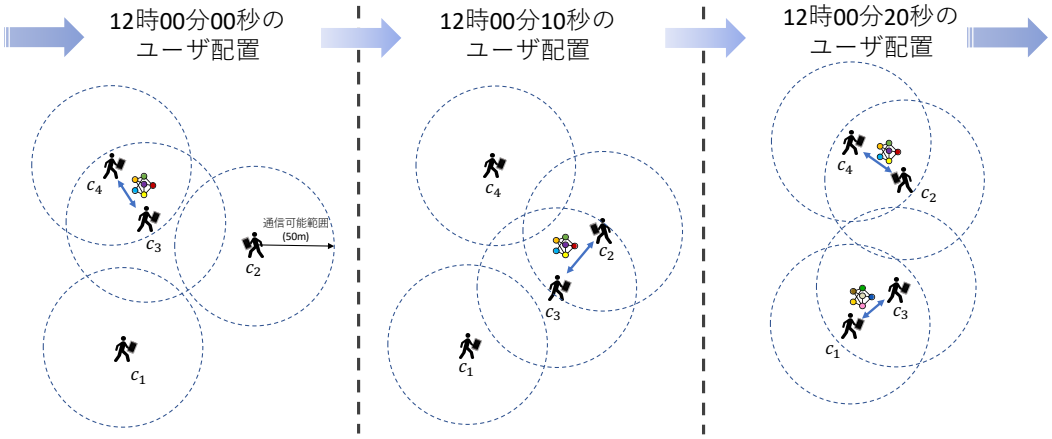



図 3: シミュレーション実験の概要

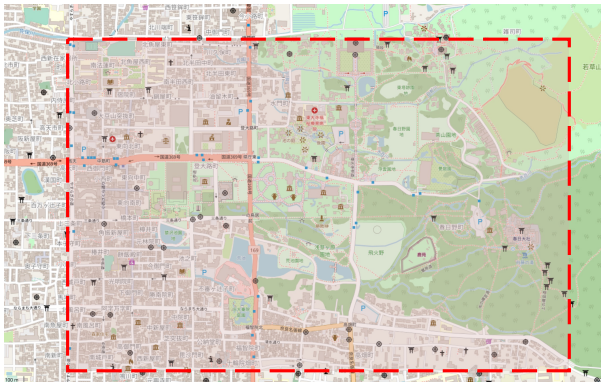


図 4: シミュレーション範囲

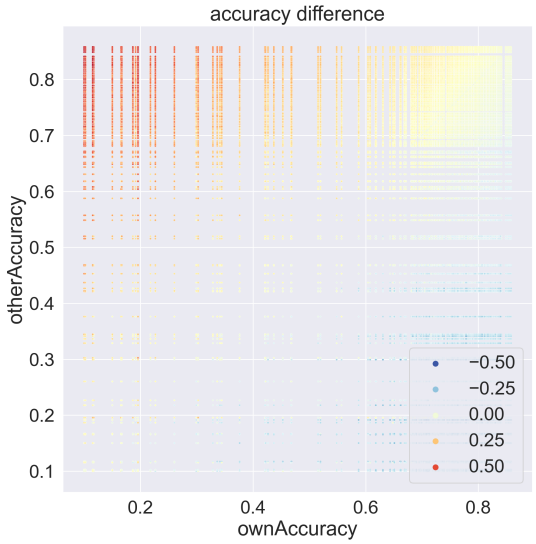



図 5: 先行研究 [4] の実験結果における精度変化度合い

上を，向上・低下・変化なしの 3 種類で表現した散布図を示していた．本稿では，**図 5** に示すような，自身のモデルに相手のモデルを統合した際の精度の差分を利用する．ownAccuracy が自分のモデル精度，otherAccuracy がコンタクト相手のモデル精度となっており，これらの差が大きい程統合後の精度変化が大きく見られる．図 5 の精度変化データに基づいて，自分と相手のモデル精度から統合後の自分のモデル精度の変化を予測するサポートベクタ回帰モデルを構築した．この回帰モデルの性能評価のために，牛や海等の 100 種類のオブジェクトを含む画像データセット cifar100[*4]から**表 2** に示す 3 パターンの 10 種類のオブジェクトのデータセットを抽出し，先行研究 [4] と同様のモデル統合実験を行い**図 6** に示す精度変化データを回帰モデル評価用として使用した．評価指標として平均絶対誤差 (MAE) を使用しており，構築した回帰モデルを各パターンで評価した結果，パターン 1 では 5.249%，パターン 2 では 5.393%，パターン 3 では 5.860%となった．

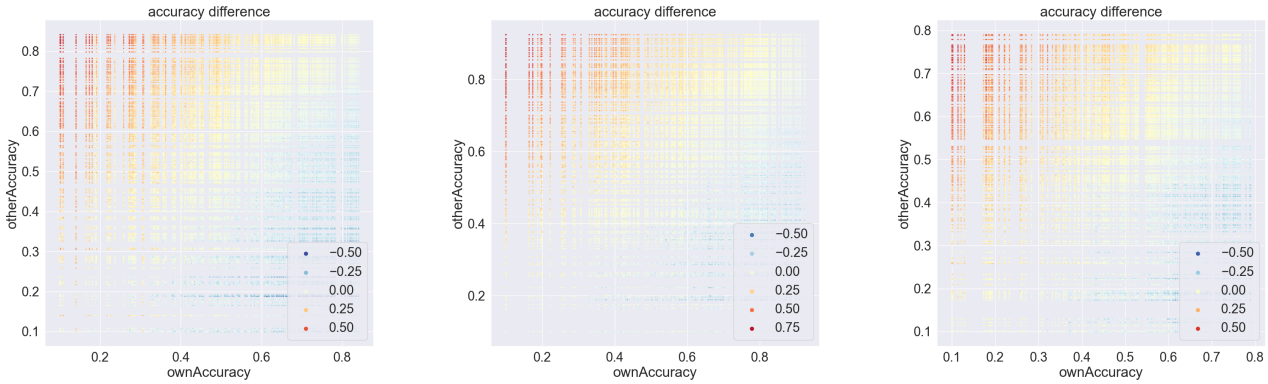
### 5.4 各ユーザへのモデル割り当て

シミュレーションでは 1,900 人分のモデルを構築した．本実験で使用したモデルは，先行研究 [4] と同様の VGG16 モデルである．cifar10 の 60,000 枚の画像から 50,000 枚を学習用とし，重複が無いように各モデルに学習データを分配した．残りの 10,000 枚の画像は，シミュレーション後の各モデルの精度評価に使用した．また，実環境においては数枚の画像を持つユーザが多数を占めることが予想される．各モデルへのデータ分配は，少ないデータを持つ人程その人数が多く，反対に多くのデータを持つユーザ程少なくなるようにした．データ分配後にモデルを学習・評価した結果，各モデルの精度は**図 7** の分布となった．図 7 より，全体で 10%〜15%の精度のモデルが多くなり，これらをシミュレーションでの初期モデルとした．

### 5.5 シミュレーション結果

各パターンのシミュレーション実験の結果，各ユーザのモデルの精度分布は**図 8** の分布となった．**図 8a** より，ゴ

[*4] https://www.cs.toronto.edu/ kriz/cifar.html




(a) パターン 1 での統合結果　(b) パターン 2 での統合結果　(c) パターン 3 での統合結果

図 6: 各パターンのオブジェクト認識モデルの精度変化度合い

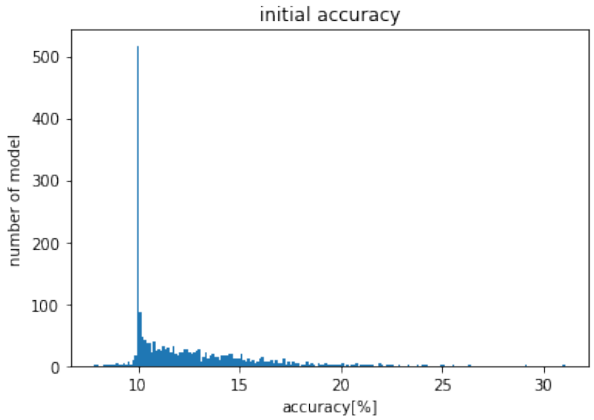



図 7: シミュレーション前の精度に対するモデルの分布

シップ手法でモデル更新を実施した場合，全モデルの平均精度は 12.45%となり，図 7 のシミュレーション前の平均精度 12.22%に対して 1.88%の精度向上が見られた．また，初期モデルの最大精度は 31.04%であるのに対し，シミュレーション後のモデルの最大精度は 22.41%に低下した．一方で，本提案手法を適用した結果は，**図 8b** より平均精度が 33.24%となり，シミュレーション前の平均精度の 172%向上した．モデルの最大精度も 35.99%となり，平均精度・最大精度共に初期モデルを上回った．

## 6. 考察

本章では，前章のシミュレーション実験で得た結果について考察する．

### 6.1 精度変化予測モデルの効果

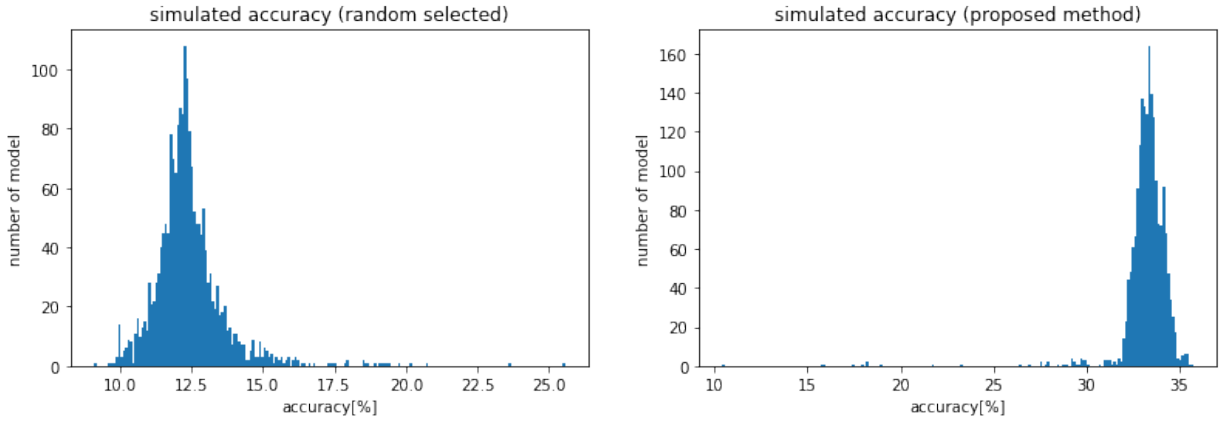
本シミュレーション実験では，2 つの手法のシミュレーションにおいて精度変化予測モデルを使用したパターンと使用しなかったパターンに分けられる．両パターンともモデルの重みパラメタの単純平均でモデルを更新したが，シミュレーション後の平均精度は，精度変化予測モデルを活用したパターン (本提案手法) が 20.79%高い結果となった．本提案アルゴリズムにおいて精度変化予測モデルは，モデル向上に有効な相手を選択するために使用していた．ゴシップ手法の場合と比較し最終的に得られた平均精度が向上していたことから，シミュレーションにおいて，精度変化予測モデルによって各モデルの精度向上に有効なモデル選択が行われていたと考える．

### 6.2 モデル精度の最大値の変化

初期モデルの最大精度は 31.04%であり，ランダムでコンタクトを選択した場合は 25.55%に低下し，提案アルゴリズムの場合は 35.99%に向上した．図 7 より，精度が低いモデルほどその数が多いため，ランダムにモデル更新すると高精度のモデルが低い精度のモデルを多く統合し，その精度を低くしたと考える．しかし，提案アルゴリズムにおいては，モデル統合後の精度が向上する可能性のあるモデルを選択する．そのため，自身の精度を低下させるモデルとの統合は比較的に発生しなかったと考える．モデル全体に対して継続した精度向上が行われたため，シミュレーション後の最大精度が向上したと考える．

## 7. おわりに

本稿では，観光客の所持データを使った観光オブジェクト認識モデル構築の手法を提案した．提案手法では観光客の所持データに含まれるプライバシ情報を保護しながらそれらの学習を行うために，Federated Learning に基づくモデル更新手法を採用した．具体的には，観光客のコンタクトが生じた時に相互端末がモデルの重みパラメタを通信し単純平均での統合後，そのパラメタを自身のモデル内に適用する手法である．また，通信回数削減のために統合後の精度変化を予測し，向上が見込まれる相手に対してのみ重みパラメタを通信するアルゴリズムを提案した．シミュレーション実験では，本提案手法とランダムにモデルを更




(a) ゴシップ手法で更新した結果　　(b) 本提案手法を適用した結果

図 8: シミュレーション後の精度に対するモデルの分布

新する手法でシミュレーションを実施し，最終的な精度の平均で評価した．結果としては，ランダムで更新する手法では 12.45%，本提案手法では 33.24%となり，シミュレーション前のモデルの平均精度が 12.22%だった点を考慮すると，提案手法を適用した場合の精度向上が大きく見られた．この結果より，事前にパラメタ統合後の精度を予測することで，限定された通信回数の下で精度向上に効果的なモデルの選択が可能になると考える．

本シミュレーションでは全体的に精度の低いモデルを使用したため，高い精度のモデルがシミュレーション環境に含まれた場合の検証も必要となる．今後は，高精度モデルの追加や観光客数の変更等，様々な条件におけるシミュレーションを実施し，本提案手法の効果を検証する．

## 謝辞

本研究は JSPS 科研費 JP21H03431 の助成を受けたものです．

### 参考文献

[1] 国土交通省観光庁. AI(人工知能) 等導入による旅行サービスの高度化事業調査報告書. https://www.mlit.go.jp/kankocho/content/001330607.pdf, 2019. Accessed: 2021-03-12.

[2] BOLDRIGHT. Deaps. https://deaps.com. Accessed: 2021-07-15.

[3] Ulrike Gretzel, Marianna Sigala, Zheng Xiang, and Chulmo Koo. Smart tourism: foundations and developments. *Electronic markets*, Vol. 25, No. 3, pp. 179–188, 2015.

[4] 冨田周作, 中村優吾, 諏訪博彦, 安本慶一ほか. 観光オブジェクト認識モデルのユーザ参加型構築手法の提案. DICOMO2021 論文集.

[5] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20 th International Conference on Artificial Intelligence and Statistics (AISTATS)*, Vol. 54, , 2017.

[6] Sangsu Lee, Xi Zheng, Jie Hua, Haris Vikalo, and Christine Julien. Opportunistic federated learning: An exploration of egocentric collaboration for pervasive computing applications. In *2021 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 1–8, 2021.

[7] Sohei Itahara, Takayuki Nishio, Yusuke Koda, Masahiro Morikura, and Koji Yamamoto. Distillation-based semi-supervised federated learning for communication-efficient collaborative training with non-iid private data. *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[8] Mingzhe Chen, H Vincent Poor, Walid Saad, and Shuguang Cui. Wireless communications for collaborative federated learning in the internet of things. *IEEE Communications Magazine*, Vol. 58, No. 12, pp. 48–54, 2020.

[9] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, Vol. 10, No. 2, pp. 1–19, 2019.

[10] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. Blockchained on-device federated learning. *IEEE Communications Letters*, Vol. 24, No. 6, pp. 1279–1283, 2019.

[11] 冨田周作, 中村優吾, 諏訪博彦, 安本慶一. Federated learning over dtn によるオブジェクト認識モデルの地域間での共有手法の検討. 2020 年度 情報処理学会関西支部 支部大会 講演論文集, Vol. 2020, , 2020.

[12] Agoop サービス製品. https://www.agoop.co.jp. Accessed: 2021-07-15.